REMARKS

Claims 1-38 are pending in this application. By this Amendment, the specification and claims 1, 4, 5, 7, 8, 11-14, 20, 21, 24-26, 28 and 33 are amended. Claims 1, 5, 7, 20, 21, 24-26, 28 and 33 are amended to recite features supported in the specification at, for example, page 13, lines 17-25. Claims 4, 8, 11-14 and 25 are amended to correct informalities. No new matter is added by any of these amendments.

Reconsideration based on the following remarks is respectfully requested.

I. Amendment Entry after Final Rejection

Entry of this amendment is proper under 37 CFR §1.116 because the amendments: a) place the application in condition for allowance (for all the reasons discussed herein); b) do not raise any new issues requiring further search or consideration; c) place the application in better condition for appeal (if necessary); and d) address formal requirements of the Final Rejection and preceding Office Action. Accordingly, Applicant respectfully requests entry of this Amendment.

II. The Claims Satisfy the Requirements under 35 U.S.C. §112, second paragraph

The Final Office Action rejects claims 1, 5, 7, 20, 21, 24-26, 28 and 33 under 35 U.S.C. §112, second paragraph, as being indefinite. Claims 1, 5, 7, 20, 21, 24-26, 28 and 33 have been amended to obviate this rejection in view of the Examiner's helpful comments. Withdrawal of the rejection under 35 U.S.C. §112, second paragraph is respectfully requested.

III. Claims 1-38 Define Patentable Subject Matter

A. The Final Office Action rejects claims 1, 2, 5-10, 19 and 20 under 35 U.S.C. §103(a) over U.S. Patent 6,154,541 to Zhang in view of U.S. Patent 5,768,382 to Schneier *et al.* (identified in the Final Office Action as Walker, and hereinafter referenced as "Schneier '382") and U.S. Patent 6,625,295 to Wolfgang *et al.* (hereinafter "Wolfgang"). This rejection is respectfully traversed.

A *prima facie* case of obviousness for a §103 rejection requires satisfaction of three basic criteria: there must be some suggestion or motivation either in the references or knowledge generally available to modify the references or combine reference teachings, a reasonable expectation of success, and the references must teach or suggest all the claim limitations (MPEP §706.02(j)). Applicant asserts that the Final Office Action fails to satisfy these requirements with Zhang, Schneier '382 and Wolfgang.

Zhang, Schneier '382 and Wolfgang, alone or in combination, do not teach or suggest a method for generating a one-way function dependent on a one-way function H and a unique value d for a user, including holding in memory a function generation unique value s by a center for the user, creating a value generation unique value u in a calculation unit from the function generation unique value s provided from the memory and the unique value d, the value generation unique value u being provided to a token for the user, and creating a one-way function value X(M) of a message M by applying the one-way function H to the value generation unique value u from the calculation unit and the message M, as recited in claim 1, and similarly recited for a device for generating one-way function values in claim 5, for a certificate issuing device in claim 24 and for an access ticket issuing device in claim 28.

Nor do Zhang, Schneier '382 and Wolfgang, alone or in combination, teach or suggest a proving device for performing processing based on a private key for a user dependent on a message M, including means for inputting the message M, means for holding a value generation unique value u for the user, means for creating a one-way function value X(M) of the message M by applying a one-way function H to the value generation unique value u from the holding means and the message M, and means for performing processing based on the one-way function value X(M), wherein the value generation unique value u is created from a function generation unique value s being held and provided by a center and a unique value d for the user, the value generation unique value u being provided to a token for the user, as recited in claim 7, and similarly recited for a device for issuing a proving instrument

T in claim 20, for an authentication device in claim 25 and for an authentication device in claim 33.

Zhang, Schneier '382 and Wolfgang, alone or in combination, also fail to teach or suggest an authentication method by which a right issuer issues rights to right recipients in association with a message M and a right verifier verifies the rights of the right recipients, wherein the right issuer creates a value generation unique value u from a function generation unique value s being held and provided by a center and a unique value d for the user corresponding to the right recipients, the value generation unique value u being provided to corresponding tokens for the right recipients; calculates a one-way function value X(M) of the message M by applying a one-way function H to the value generation unique value u from the right issuer and the message M; and issues an access ticket t determined from a private key x and the one-way function value X(M) to the right recipients, as recited in claims 21 and 26.

Instead, Zhang discloses a cryptographic system that encrypts a ciphertext C by a key vector K_c. In particular, Zhang teaches loading data bits into a data register 41, resetting a code register 42, shifting bits by a shifter 43 and fed to a multiplier 45 (col. 14, lines 11-60 and Fig. 4 of Zhang). Also, Zhang teaches encryption key schemes including PPKS and QPKS using an invertable permuter P, as well as constructions methods such as RPKM, SPKM, WPKM, CLLM, VLLM, UVOTP, BFSM and EDBM (col. 15, lines 18-42, col.18, lines 1-22, col. 19, lines 24-36, col. 22, lines 48-53, col. 23, lines 31-43 of Zhang). Such teachings are unrelated to the value generation and function generation unique values in conjunction with the user's token, as provided in Applicant's independent claims.

The Final Office Action admits on page 5 (paragraph 15) that Zhang does not disclose "combining a unique value d and a unique value s to create the unique value u", but asserts that Zhang teaches strategies combining parameters to generate new parameters (col. 21, line 65 – col. 22, line 36 of Zhang). Thus, the Final Office Action asserts that it would have been obvious to use the strategies in Zhang to achieve creating a value generation unique value u from the function generation unique value s and the unique value d, as recited in Applicant's claimed combination of features. Applicant respectfully disagrees, and asserts that generalized combinations of parameters fails to have rendered obvious to one of ordinary skill in the art, absent hindsight, the unique values recited in Applicant's claimed combination of features, including use of a one-way function to calculate the value generation unique value u.

Further, Schneier '382 discloses protocols for coding and encoding messages on game outcomes. In particular, Schneier '382 teaches a central computer 12 associated with game computers 14 operating game software 15 in memory 23. Schneier '382 further teaches encrypting an outcome message by a game computer 14 with a public-key/private-key pair to form an authentication outcome message (AOM), and accepting the AOM by the central computer 12 using signature verification and the public key (col. 5, lines 29-56, col. 10, lines 27-56 and Figs. 1A and 5 of Schneier '382). Although Schneier '382 discloses use of "tokens", these constitute physical computing devices, and thus their context differs from Applicant's claimed combination of features as a tamper-resistant enclosure for a private key.

Also, Wolfgang discloses a method of signal authentication by applying a watermark. In particular, Wolfgang teaches a watermark 50 incorporated in an original image 52 by an algorithm 54 to produce a watermarked image 56 (col. 6, lines 33-37 and Fig. 2 of Wolfgang).

Further, there would have been no motivation to combine features related to the databit manipulation of Zhang with the game message encoding protocol of Schneier '382 and the signal watermarks of Wolfgang, nor has the Final Office Action established sufficient motivation for a *prima facie* case of obviousness. Even assuming that motivation to combine the applied references is established, the combination fails to teach or suggest Applicant's claimed combination of features.

B. The Final Office Action further rejects claims 18, 21-30 and 33 under 35 U.S.C. §103(a) over Zhang in view of Schneier '382 and Wolfgang and further in view of *Cryptography and Network Security*, 2/e by Stallings. The Final Office Action further rejects claims 3, 4 and 11-17 under 35 U.S.C. §103(a) over Zhang in view of Schneier '382 and Wolfgang and further in view of *Applied Cryptography*, 2/e by Schneier (hereinafter "Schneier *AC*"). The Final Office Action further rejects claims 31, 32 and 34-38 under 35 U.S.C. §103(a) over Zhang in view of Schneier '382, Wolfgang, Stallings and Schneier *AC*. These rejections are respectfully traversed.

Stallings and Schneier *AP* do not compensate for the deficiencies of Zhang, Schneier '382 and Wolfgang outlined above for claims 1 and 7. Nor does Stallings teach, disclose or suggest the additional features recited in claims 18, 21-30 and 33. Also, Schneier *AC* fails to teach, disclose or suggest the additional features recited in claims 3, 4 and 11-17. Further, Stallings and Schneier *AC* do not teach, disclose or suggest the additional features recited in claims 31, 32 and 34-38.

Applicant asserts that the Final Office Action fails to satisfy the requirements for a *prima facie* case of obviousness with Zhang, Schneier '382, Wolfgang, Stallings and/or Schneier *AC*. In particular, Stallings discloses certificate authentication. In particular, Stallings teaches the X.509 scheme procedures (§11.2 of Stallings). In addition, Schneier *AC* discloses encryption and decryption protocols. In particular, Schneier *AC* teaches algorithm complexity comparison and describes the DES block cipher (§§11.2, 12.2 of Schneier *AC*).

Further, there would have been no motivation to combine features related to the databit manipulation of Zhang with the game message encoding protocol of Schneier '382, the signal watermarks of Wolfgang, the authentication procedures of Stallings and the cryptographic protocols of Schneier *AC*, nor has the Final Office Action established sufficient motivation for a *prima facie* case of obviousness. Even assuming that motivation to combine the applied references is established, the combinations fail to teach or suggest Applicant's claimed combination of features.

The Final Office Action admits on page 8 (paragraph 22) that Zhang does not teach or suggest "the message M including the use conditions of the message by the method", but asserts that Stallings teaches use conditions for X.509 certificates. The Final Office Action further asserts that motivation for combining these teachings would have been to enable distribution of several types of messages. Applicant respectfully disagrees and asserts that employing use conditions for a certificate C has no bearing on use conditions for a message M, as recited in claim 18. The certificate provides means to prove a public key y in Stallings. In contrast, the message M can include processing parameters, such as a finite Abelian (*i.e.*, commutative) group G, a prime number p, mappings π, ε, η, and a homomorphism g. Therefore, the use conditions for message M cannot be considered analogous to such techniques applied to the certificate.

The Final Office Action admits on page 10 (paragraph 28) that Zhang does not disclose "the access ticket being calculated as a difference between the private key x and the generated private key [amended to one-way function value] X(M) nor the quotient x/X(M)", but asserts that differences or quotients are typically mathematical operations to determine equality of two values. Applicant respectfully disagrees, and asserts that the modulo operation implied by such expressions is not analogous to comparisons between the issued private key and the calculated one-way function value of Applicant's claimed combination of features for claims 29 and 30, and that there would have been no motivation to apply such mathematical operations to the databit manipulation procedures in Zhang.

The Final Office Action admits on page 11 (paragraph 30) that Zhang does not teach "an encryption function with a symmetric key as the scrambling operation", but asserts that Schneier *AC* teaches scrambling techniques, and that applying these teachings to Zhang would have been obvious. Applicant respectfully disagrees, and asserts that scrambling with a symmetric key has no relationship with producing a random number k, calculating a commitment w from the random number k, and calculating a response r from an input challenge c, a one-way function value X(M), the random number k and the commitment w, as recited in Applicant's combination of features in claim 3.

The Final Office Action admits on page 11 (paragraph 31) that Zhang does not disclose "calculating X(M) by applying both the one-way function H and an encryption function D [amended to E] of a symmetry key to the values of u and M", but that asserts that encryption using symmetric keys are efficient means to hide sensitive values, as taught in Schneider *AC*, and that such a combination would have been obvious. Applicant respectfully disagrees, and asserts that the symmetric key scrambling would not have rendered obvious applying a one-way function H and an encryption function E of a symmetric key to the value u and the message M, as recited in Applicant's combination of features in claim 4.

The Final Office Action admits on page 13 (paragraph 33) that Zhang fails to teach "combining two values" as bit concatenation, but asserts that such operations are typical when values are of differing sizes, such as in DES. Applicant respectfully disagrees, and asserts that by applying encryption to game machine accounting, Zhang lacks any teaching for bit concatenation, as provided in Applicant's combination of features in claims 31 and 32.

The Final Office Action admits on page 13 (paragraph 34) that Zhang does not disclose "using the access ticket to update values used in authentication", but asserts that such difference or quotient teachings would have been obvious constructions to show equality or inequality of two values. Applicant respectfully disagrees, and asserts that Zhang lacks any teaching or suggestion to update values or to use access tickets in authentication, as provided in Applicant's combination of features in claims 34-38.

For at least these reasons, Applicant respectfully asserts that the independent claims are now patentable over the applied references. The dependent claims are likewise patentable over the applied references for at least the reasons discussed as well as for the additional features they recite. Consequently, all the claims are in condition for allowance. Thus, Applicant respectfully requests that the rejections under 35 U.S.C. §103 be withdrawn.

IV. Conclusion

In view of the foregoing amendments and remarks, Applicant respectfully submits that this application is in condition for allowance. Favorable reconsideration and prompt allowance are earnestly solicited.

Should the Examiner believe that anything further is desirable in order to place this application in even better condition for allowance, the Examiner is invited to contact Applicant's undersigned representative at the telephone number listed below.

Respectfully submitted,

James A. Oliff
Registration No. 27,075

Gerhard W. Thielman
Registration No. 43,186

JAO:GWT/gwt

Date: November 12, 2004

OLIFF & BERRIDGE, PLC
P.O. Box 19928
Alexandria, Virginia 22320
Telephone: (703) 836-6400

DEPOSIT ACCOUNT USE
AUTHORIZATION
Please grant any extension
necessary for entry;
Charge any fee due to our
Deposit Account No. 15-0461